

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Luke D. Jagger et al.

Application No.: 10/072,708

Group No.: 2143

Filed: 02/05/2002

Examiner: Bilgrami, A.

For: SPAM REPORT GENERATION SYSTEM AND METHOD

Mail Stop Appeal Briefs – Patents

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF  
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. This brief is in furtherance of the Notice of Appeal filed August 3, 2006, a substitute for the Appeal Brief filed December 11, 2006, and in response to the Notification of Non-Compliant Appeal Brief mailed on February 8, 2007.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. §1.17(c), the fee for filing the Appeal Brief has already been paid. However, the Commissioner is authorized to charge any fees that may be due to deposit account 50-1351 (NAHP314).

4. EXTENSION OF TERM

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	\$0.00 (previously paid on December 11, 2006)
Extension fee (if any)	\$0.00
<b>TOTAL FEE DUE</b>	<b>\$0.00</b>

6. FEE PAYMENT

Applicant believes that only the above fees are due in connection with the filing of this paper because the appeal brief was paid with a previous submission. However, the Commissioner is authorized to charge any additional fees that may be due (e.g. for any reason including, but not limited to fee changes, etc.) to Deposit Account No. 50-1351 (Order No. NA11P314).

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NA11P314).

/KEVINZILKA/

Reg. No.: 41,429  
Tel. No.: 408-971-2573  
Customer No.: 28875

Signature of Practitioner  
Kevin J. Zilka  
Zilka-Kotab, PC  
P.O. Box 721120  
San Jose, CA 95172-1120  
USA

**PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	)	
	)	
Jagger et al.	)	Group Art Unit: 2143
	)	
Application No. 10/072,708	)	Examiner: Bilgrami, Asghar H.
	)	
Filed: February 5, 2002	)	Date: March 8, 2007
	)	
For: SPAM REPORT GENERATION SYSTEM	)	
AND METHOD	)	
	)	
	)	

---

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**ATTENTION: Board of Patent Appeals and Interferences**

**SUBSTITUTE APPEAL BRIEF (37 C.F.R. § 41.37)**

This brief is in furtherance of the Notice of Appeal filed August 3, 2006, a substitute for the Appeal Brief filed December 11, 2006, and in response to the Notification of Non-Compliant Appeal Brief mailed on February 8, 2007 (see attached). While appellant disagrees with the Examiner as to whether the alleged deficiencies exist in the original Appeal Brief, a Substitute Appeal Brief with appropriate edits is nevertheless submitted to expedite prosecution.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

- I REAL PARTY IN INTEREST
- II RELATED APPEALS AND INTERFERENCES

III	STATUS OF CLAIMS
IV	STATUS OF AMENDMENTS
V	SUMMARY OF CLAIMED SUBJECT MATTER
VI	GROUND OF REJECTION TO BE REVIEWED ON APPEAL
VII	ARGUMENT
VIII	CLAIMS APPENDIX
IX	EVIDENCE APPENDIX
X	RELATED PROCEEDING APPENDIX

The final page of this brief bears the practitioner's signature.

**I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))**

The real party in interest in this appeal is McAfee, Inc.

## **II. RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))**

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

A Related Proceedings Appendix is appended hereto.

**III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))**

**A. TOTAL NUMBER OF CLAIMS IN APPLICATION**

Claims in the application are: 1-8, and 10-31

**B. STATUS OF ALL THE CLAIMS IN APPLICATION**

1. Claims withdrawn from consideration: None
2. Claims pending: 1-8, and 10-31
3. Claims allowed: None
4. Claims rejected: 1-8, and 10-31
5. Claims cancelled: 9

**C. CLAIMS ON APPEAL**

The claims on appeal are: 1-8, and 10-31

See additional status information in the Appendix of Claims.

**IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))**

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.



## **V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))**

With respect to a summary of Claim 1, as shown in Figure 4 et al., a method is provided for generating a report on an unsolicited electronic message. In use, an electronic mail message is received (e.g. see item 80 of Figure 4, etc.). Further, it is determined whether the electronic message is an unsolicited message (e.g. see item 82 of Figure 4, etc.), and if the message is an unsolicited message, the message is examined to identify a network address relating to the message (e.g. see item 84 of Figure 4, etc.). In addition, an authority hosting the network address is identified (e.g. see item 86 of Figure 4, etc.), and a report containing the identified network address and hosting authority is generated (e.g. see item 88 of Figure 4, etc.). Moreover, identifying the hosting authority comprises identifying an owner of a network domain. See, for example, page 4, line 2 – page 5, line 14 et al.

With respect to a summary of Claim 2, as shown in Figure 4 et al., the generated report is transmitted to the identified hosting authority (e.g. see item 100 of Figure 4, etc.). See, for example, page 4, lines 6-8; and page 4, lines 10-12 et al.

With respect to a summary of Claim 4, identifying a URL comprises comparing text within the electronic message to a database of words to identify the URL. See, for example, page 5, lines 3-4; page 11, lines 1-4; and page 11, line 19 – page 12, line 2 et al.

With respect to a summary of Claim 5, the identified URL is compared to a database of legitimate URLs. See, for example, page 5, lines 5-6; and page 12, lines 9-15 et al.

With respect to a summary of Claim 10, identifying the hosting authority comprises identifying an Internet service provider. See, for example, page 12, lines 9-10; page 12, lines 13-14; and page 14, lines 1-7 et al.

With respect to a summary of Claim 11, the report is transmitted to a central managed service provider configured to forward the report to the identified hosting authority. See, for example, page 17, lines 13-15 et al.

With respect to a summary of Claim 12, at least temporarily saving the report and transmitting the report to the identified hosting authority at the end of a specified period. See, for example, page 17, lines 15-17 et al.

With respect to a summary of Claim 13, as shown in Figure 2 et al., a system is provided for generating a report on an unsolicited electronic message. A detector (e.g. see item 44 of Figure 2, etc.) is included that is operable to detect a network address within an electronic message identified as an unsolicited message. Further, a host identifier (e.g. see item 48 of Figure 2, etc.) is included that is operable to identify an authority hosting the network address. In addition, a report generator (e.g. see item 50 of Figure 2, etc.) is included that is operable to generate a report containing the identified network address and hosting authority. A storage medium (e.g. see item 46 of Figure 2, etc.) is included that is configured to at least temporarily store the identified network address and hosting authority. Moreover, identifying the hosting authority comprises identifying an owner of a network domain. See, for example, page 4, line 2 – page 5, line 14 et al.

With respect to a summary of Claim 16, the hosting authority is an Internet service provider. See, for example, page 12, lines 9-11 et al.

With respect to a summary of Claim 18, as shown in Figure 4 et al., the processor is configured to transmit the report to the identified hosting authority (e.g. see item 100 of Figure 4, etc.). See, for example, page 4, lines 6-8; and page 4, lines 10-12 et al.

With respect to a summary of Claim 19, the processor is configured to transmit the report to a central managed service provider. See, for example, page 17, lines 13-15 et al.

With respect to a summary of Claim 20, a database containing search terms is used to identify the network address within text of the electronic message. See, for example, page 11, line 19 – page 12, line 2 et al.

With respect to a summary of Claim 21, a database contains a list of trusted network addresses. See, for example, page 12, lines 3-5 et al.

With respect to a summary of Claim 22, as shown in Figure 4 et al., a computer product is provided for generating a report on an unsolicited electronic message. Code is included that receives an electronic mail message (e.g. see item 80 of Figure 4, etc.). Further, the code is included that determines whether the electronic message is an unsolicited message (e.g. see item 82 of Figure 4, etc.). In addition, code is included that examines the message to identify a network address relating to the message if the message is an unsolicited message (e.g. see item 84 of Figure 4, etc.). Furthermore, code is included that identifies an authority hosting the network address (e.g. see item 86 of Figure 4, etc.), and that generates a report containing the identified network address (e.g. see item 88 of Figure 4, etc.). Also included is a computer readable medium that stores said computer codes. Moreover, identifying the hosting authority comprises identifying an owner of a network domain. See, for example, page 4, line 2 – page 5, line 14 et al.

With respect to a summary of Claim 24, as shown in Figure 4 et al., code transmits the generated report to the identified hosting authority (e.g. see item 100 of Figure 4, etc.). See, for example, page 4, lines 6-8; and page 4, lines 10-12 et al.

With respect to a summary of Claim 25, code compares text within the electronic message to a database of words to locate the network address within the text. See, for example, page 11, lines 1-4; and page 11, line 19 – page 12, line 2 et al.

With respect to a summary of Claim 26, code compares the identified network address with trusted network addresses. See, for example, page 11, line 19 – page 12, line 5 et al.

With respect to a summary of Claim 29, the report is utilized to generate an electronic mail message to be sent to the identified organization. See, for example, page 12, line 18 – page 13, line 21 et al.

With respect to a summary of Claim 30, identifying the URL further comprises examining text surrounding the URL to determine a likelihood that the URL is an address of a web site associated with unsolicited messages. See, for example, page 11, lines 13-15 et al.

With respect to a summary of Claim 31, the report includes disclaimer information and user definable text. See, for example, page 14, lines 15-16 et al.

Of course, the above citations are merely examples of the above claim language and should not be construed as limiting in any manner.

**VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. §  
41.37(c)(1)(vi))**

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claims 1-8, and 10-31 under 35 U.S.C. 103(a) as being unpatentable over Aronson et al. (U.S. Patent No. 6,654,787 B1), in view of Leeds (U.S. Patent No. 6,393,465 B2).

## VII ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

### Issue # 1:

The Examiner has rejected Claims 1-8, and 10-31 under 35 U.S.C. 103(a) as being unpatentable over Aronson et al. (U.S. Patent No. 6,654,787 B1), in view of Leeds (U.S. Patent No. 6,393,465 B2).

#### *Group #1: Claims 1, 3, 7-8, 13-15, 17, and 27-28*

With respect to such claims, the Examiner has relied on Col. 4, lines 51-56; Col. 5, lines 50-67; and the Abstract in Aronson along with Col. 3, lines 54-67; and Col. 4, lines 1-35 in Leeds to make a prior art showing of appellant's claimed "identifying an authority hosting the network address" (see the same or similar, but not necessarily identical language in the foregoing claims).

Appellant respectfully asserts that the excerpts from Leeds relied on by the Examiner only relate to a host computer associated with a sender of an electronic mail message (see Abstract and Col. 4, lines 66-67, specifically). In addition, Leeds discloses that "if a message has purportedly been relayed through a machine named mail.fromnowhere.com and the mail handling system has determined that such a machine does not actually exist, the confidence rating for the message should be increased." Clearly, determining a host computer/host name of a sender of e-mail or relay, as in Leeds, does not meet appellant's specific claim language, namely an "authority hosting the network address" (emphasis added), as claimed by appellant.

Further, appellant respectfully asserts that the excerpts from Aronson relied upon by the Examiner merely disclose that "[o]ther contemplated rule handling filter modules will filter e-mail based on: (1) word or letter frequency analysis; (2) IP source frequency analysis; (3) misspelling analysis (unwanted e-mail often contains misspelled words); (4) word or letter combination analysis; (5) technical or legal RFC822 header compliance; and (6) feature

extraction & analysis (e.g., based on phone numbers, URL's, addresses, etc.)" (emphasis added). Clearly, filtering e-mail based on IP source frequency and feature extraction & analysis fails to even suggest "identifying an authority hosting the network address" (emphasis added), as claimed by appellant.

In addition, the Examiner argued that "Ar[on]son disclosed that the source header data from an incoming e-mail address (aardvark@aol.com) is analyzed by the spam probes." Further, the Examiner argued that "[t]he source header data includes the ISP (in this case "aol") hosting the spammer's network address (see col.4, lines 45-67)." Appellant disagrees and respectfully asserts that the excerpt from Aronson simply discloses that "[a] spam probe is an e-mail address selected to make its way onto as many spam mailing lists as possible." Aronson continues, teaching that "[i]t is also selected to appear high up on spammers' lists in order to receive spam mailings early in the mailing process" using an e-mail address such as "aardvark@aol.com." Clearly, the mere disclosure of using an e-mail address in a spam probe, as in Aronson, completely fails to even suggest "identifying an authority hosting the network address" (emphasis added), as claimed by appellant.

Still with respect to the present claims the Examiner has again relied on the Abstract, Col. 3, lines 54-67, and Col. 4, lines 1-35 in Leeds to make a prior art showing of appellant's claimed "generating a report containing the identified network address and hosting authority" (see the same or similar, but not necessarily identical language in foregoing claims).

Appellant respectfully asserts that the only suggestion of a "report" in the excerpts relied on by the Examiner merely relates to "seed addresses [which] can alert an e-mail provider to potential mass mailings by reporting when mail is received for ghost or non-existent accounts." Clearly, alerting an e-mail provider when an e-mail is received for a seed address, as in Leeds, fails to even suggest "generating a report containing the identified network address and hosting authority" (emphasis added), as claimed by appellant.

Further, the Examiner argued that "Leeds also describes the similar process of identifying the host name of the spammer's address (please see col.4, lines 60-67 & col.5, lines 1-45)." Appellant disagrees and respectfully asserts that Leeds simply discloses that "[t]he fields for

"Return Path:," "From:," and "Reply-To:" are highlighted as three of the fields which the present invention will parse from the message header.' As an example, Leeds teaches that "From: 48941493@notarealaddress.com is broken down into a user id (48941493) and a host name (notarealaddress.com)" (emphasis added). Leeds continues, disclosing that 'a first level check is [used] to determine if the alleged sender identified by the "From:" or "Reply-To:" fields are valid.' Moreover, Leeds discloses that the first level check 'includ[es]: (1) sending a message to the user identified by the "From:" or "Reply-To:" fields and examining whether the message can be successfully delivered, (2) using the UNIX "whois" command to determine if a site (or host) by that name actually exists, (3) using the UNIX "finger" command to identify if a user name exists at a verifiable host, (4) using the "vfry" command when connected to a sendmail daemon to verify that a user exists at a particular site, and (5) using the UNIX "traceroute" command to make sure there is a valid route back to the specified host' (emphasis added). Clearly, performing a first level check including using whois, and traceroute to verify the host name from the "From:" and "Reply-To:" fields, as in Leeds, fails to even suggest "generating a report containing the identified network address and hosting authority" (emphasis added), as claimed by appellant.

Further, with respect to each of the present claims, the Examiner has relied on Col. 4, lines 60-67; Col. 5, lines 1-44, and Col. 6, lines 52-65 in Leeds to make a prior art showing of appellant's claimed technique "wherein identifying the hosting authority comprises identifying an owner of a network domain" (see the same or similar, but not necessarily identical language in the foregoing claims).

Appellant respectfully asserts that the excerpts from Leeds relied upon by the Examiner merely disclose 'a first level check is to determine if the alleged sender identified by the "From:" or "Reply-To:" fields are valid' (emphasis added). In addition, Leeds discloses 'using the UNIX "whois" command to determine if a site (or host) by that name actually exists' (emphasis added). Clearly, using whois to perform a first level check to ensure the host actually exists for the alleged sender in the "From:" or "Reply-To:" fields, as in Leeds, fails to even suggest a technique "wherein identifying the hosting authority comprises identifying an owner of a network domain" (emphasis added), as claimed by appellant. Appellant respectfully asserts that



merely ensuring that a host actually exists fails to even suggest “identifying an owner of a network domain,” as claimed by appellant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant’s disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

*Group #2: Claims 2, 18, and 24*

With respect to Claim 2 et al., the Examiner has relied on Col. 4, lines 36-67; Col. 5, lines 1-44, and Col. 8, lines 34-57 in Leeds to make a prior art showing of appellant’s claimed “transmitting the generated report to the identified hosting authority.”

Appellant respectfully asserts that the only mention of any sort of report, in such excerpts from Leeds, is the teaching that ‘addresses could be watched for incoming junk e-mail and a notification from the authentication server could then be broadcast to users indicating that mail with the subject of “XYZ” is junk e-mail’ (see, specifically, Col. 8, lines 47-50). Clearly, such notification sent to users does not meet appellant’s claimed “transmitting the generated report to the identified hosting authority” (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

*Group #3: Claim 4*

With respect to Claim 4, the Examiner has relied on Col. 4, lines 57-67; Col. 5, lines 1-8; and Col. 5, lines 50-67 in Aronson to make a prior art showing of appellant's claimed technique "wherein identifying a URL comprises comparing text within the electronic message to a database of words to identify the URL."

After careful review of the excerpts relied on by the Examiner, appellant notes that the only URL disclosed in Aronson relates to filtering e-mail based on "feature extraction & analysis (e.g.,...URL's...)" (see Col. 5, lines 63-64). However, Aronson does not teach how such URL is identified, whereas appellant specifically claims "identifying a URL [by] comparing text within the electronic message to a database of words to identify the URL," as claimed. Appellant further notes that Aronson only teaches that spam may be filtered "based on a specific keyword search," and that therefore the keywords are used to identify spam, but not that a database of words is utilized to "identify the URL," (emphasis added), in the manner claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

*Group #4: Claim 5 and 6*

With respect to Claim 5, the Examiner has relied on Col. 4, lines 57-67; Col. 5, lines 1-8; and Col. 5, lines 50-67 in Aronson to make a prior art showing of appellant's claimed "comparing the identified URL to a database of legitimate URLs."

After careful review of the excerpts relied on by the Examiner, appellant notes that Aronson merely discloses that "[i]f the network address contained in the source header is identified as the network address of a known spammer, a rule will be established to filter all incoming e-mail from this network address into the spam storage area 230" (Col. 4, lines 60-62 – emphasis added). Further, Aronson discloses that "[r]ules 210 based on keywords in the subject or body of spam e-mail may also be established" and "[f]or example, all e-mails containing the two words "sex" and "free" may be identified as spam and filtered" (Col. 4, lines 2-5 – emphasis added). In

addition, Aronson discloses that “[o]ther contemplated rule handling filter modules will filter e-mail based on: (1) word or letter frequency analysis; (2) IP source frequency analysis, (3) misspelling analysis (unwanted e-mail often contains misspelled words); (4) word or letter combination analysis; (5) technical or legal RFC822 header compliance; and (6) feature extraction & analysis (e.g., based on phone numbers, URL's, addresses, etc.)” (Col. 5, lines 58-64 – emphasis added).

However, appellant respectfully asserts that Aronson’s disclosure of filtering e-mail as spam based on keywords, the source address being identified as a known spammer, IP source frequency analysis, and feature extraction and analysis, simply fails to even suggest “comparing the identified URL to a database of legitimate URLs” (emphasis added), as claimed by appellant. Clearly, filtering based on a feature extraction and analysis of a URL fails to suggest “comparing the identified URL to a database of legitimate URLs” (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

*Group #5: Claim 10*

With respect to Claim 10, the Examiner has relied on Col. 3, lines 54-67; Col. 4, lines 1-23; Col. 4, lines 1-23 and 60-67; and Col. 5, lines 1-44; in Leeds to make a prior art showing of appellant’s claimed technique “wherein identifying the hosting authority comprises identifying an Internet service provider.”

Appellant respectfully asserts that the excerpts from Leeds relied upon by the Examiner merely disclose that “a first level check is to determine if the alleged sender identified by the “From:” or “Reply-To:” fields are valid” (emphasis added). In addition, Leeds discloses “using the UNIX “whois” command to determine if a site (or host) by that name actually exists” (emphasis added). Clearly, using whois to perform a first level check to ensure the host actually exists for the alleged sender in the “From:” or “Reply-To:” fields, as in Leeds, fails to even suggest a technique “wherein identifying the hosting authority comprises identifying an Internet service provider” (emphasis added), as claimed by appellant. Appellant respectfully asserts that merely

ensuring that a host actually exists fails to specifically suggest “identifying an Internet service provider,” in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

*Group #6: Claim 11*

With respect to Claim 11, the Examiner has relied on Col. 4, lines 36-67; Col. 5, lines 1-44; and Col. 8, lines 34-57 in Leeds to make a prior art showing of appellant’s claimed “transmitting the report to a central managed service provider configured to forward the report to the identified hosting authority.”

Appellant respectfully asserts that the only mention of any sort of report in such excerpts from Leeds simply teaches that ‘addresses could be watched for incoming junk e-mail and a notification from the authentication server could then be broadcast to users indicating that mail with the subject of “XYZ” is junk e-mail’ (see, specifically, Col. 8, lines 47-50). However, such notification sent to users does not meet appellant’s claimed “transmitting the report to a central managed service provider configured to forward the report to the identified hosting authority” (emphasis added), as claimed by appellant. Clearly, sending a notification to users, as in Leeds, fails to meet “transmitting the report to a central managed service provider” (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

*Group #7: Claim 12*

With respect to Claim 12, the Examiner has relied on Col. 5, lines 38-44 in Leeds to make a prior art showing of appellant’s claimed technique including “at least temporarily saving the report and transmitting the report to the identified hosting authority at the end of a specified period.”

Appellant respectfully asserts that such excerpt only relates to “sending a verification message...within a period of time.” Clearly, sending a verification message to determine if a user is actually associated with the sender of e-mail does not meet appellant’s claimed report, let alone “transmitting the report to the identified hosting authority at the end of a specified period” (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

*Group #8: Claim 16*

With respect to Claim 16, the Examiner has relied on Col. 3, lines 54-67; Col. 4, lines 1-23 and 60-67; and Col. 5, lines 1-44 in Leeds to make a prior art showing of appellant’s claimed technique “wherein the hosting authority is an Internet service provider.”

Appellant respectfully asserts that the excerpts from Leeds relied upon by the Examiner merely disclose that ‘a first level check is to determine if the alleged sender identified by the “From:” or “Reply-To:” fields are valid’ (emphasis added). In addition, Leeds discloses ‘using the UNIX “whois” command to determine if a site (or host) by that name actually exists’ (emphasis added). Clearly, using whois to perform a first level check to ensure the host actually exists for the alleged sender in the “From:” or “Reply-To:” fields, as in Leeds, fails to even suggest a technique “wherein the hosting authority is an Internet service provider” (emphasis added), as claimed by appellant. Appellant respectfully asserts that merely ensuring that a host actually exists fails to specifically suggest a “hosting authority [that] is an Internet service provider,” as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

*Group #9: Claim 19*

With respect to Claim 19, the Examiner has relied on Col. 4, lines 36-67; Col. 5, lines 1-44; and Col. 8, lines 34-57 in Leeds to make a prior art showing of appellant's claimed technique "wherein the processor is configured to transmit the report to a central managed service provider."

Appellant respectfully asserts that the only mention of any sort of report in such excerpts from Leeds simply teaches that 'addresses could be watched for incoming junk e-mail and a notification from the authentication server could then be broadcast to users indicating that mail with the subject of "XYZ" is junk e-mail' (see, specifically, Col. 8, lines 47-50). However, such notification sent to users does not meet appellant's claimed "transmit[ing] the report to a central managed service provider" (emphasis added), as claimed by appellant. Clearly, sending a notification to users, as in Leeds, fails to meet "transmit[ing] the report to a central managed service provider" (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

*Group #10: Claim 20*

With respect to Claim 20, the Examiner has relied on Col. 4, lines 57-67; Col. 5, lines 1-8; and Col. 5, lines 50-67 in Aronson to make a prior art showing of appellant's claimed "database containing search terms used to identify the network address within text of the electronic message"

After careful review of the excerpts relied on by the Examiner, appellant notes that Aronson merely discloses that "[i]f the network address contained in the source header is identified as the network address of a known spammer, a rule will be established to filter all incoming e-mail from this network address into the spam storage area 230" (Col. 4, lines 60-62 -- emphasis added). Further, Aronson discloses that "[r]ules 210 based on keywords in the subject or body of spam e-mail may also be established" and "[f]or example, all e-mails containing the two words "sex" and "free" may be identified as spam and filtered" (Col. 4, lines 2-5 -- emphasis added). In addition, Aronson discloses that "[o]ther contemplated rule handling filter modules will filter e-

mail based on: (1) word or letter frequency analysis; (2) IP source frequency analysis; (3) misspelling analysis (unwanted e-mail often contains misspelled words); (4) word or letter combination analysis; (5) technical or legal RFC822 header compliance; and (6) feature extraction & analysis (e.g., based on phone numbers, URL's, addresses, etc.)” (Col. 5, lines 58-64 – emphasis added).

However, Aronson’s mere disclosure that the network address contained within the source header is used by a rule to filter e-mail from this network address to a spam storage area simply fails to even suggest that “a database containing search terms [is] used to identify the network address within text of the electronic message” (emphasis added), in the manner claimed by appellant. Further, disclosing identifying and filtering spam based on keywords in the subject or body, as in Aronson, fails to suggest that “a database containing search terms [is] used to identify the network address within text of the electronic message” (emphasis added), as claimed by appellant. In addition, Aronson’s disclosure that rule handling filter modules will filter e-mail based on IP source frequency analysis, and feature extraction & analysis simply fails to suggest that “a database containing search terms [is] used to identify the network address within text of the electronic message” (emphasis added), as claimed by appellant. Clearly, identifying and filtering spam based on keywords and features, as in Aronson, fails to meet “a database containing search terms used to identify the network address” (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

#### *Group #11: Claim 21*

With respect to Claim 21, the Examiner has relied on Col. 4, lines 57-67; Col. 5, lines 1-8; and Col. 5, lines 50-67 in Aronson to make a prior art showing of appellant’s claimed “database containing a list of trusted network addresses.”

After careful review of the excerpts relied on by the Examiner, appellant notes that Aronson merely discloses that “[i]f the network address contained in the source header is identified as the

network address of a known spammer, a rule will be established to filter all incoming e-mail from this network address into the spam storage area 230" (Col. 4, lines 60-62 – emphasis added). However, appellant respectfully asserts that Aronson's disclosure of filtering e-mail as spam based on the source address being identified as a known spammer simply fails to even suggest "a database containing a list of trusted network addresses" (emphasis added), as claimed by appellant. Clearly, a source address of a known spammer, as in Aronson, simply fails to suggest "a list of trusted network addresses" (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

#### *Group 12: Claims 22 and 23*

With respect to independent Claim 22, the Examiner has relied on Col. 4, lines 51-56; Col. 5, lines 50-67; and the Abstract in Aronson along with Col. 3, lines 54-67; and Col. 4, lines 1-35 in Leeds to make a prior art showing of appellant's claimed "code that identifies an authority hosting the network address."

Appellant respectfully asserts that the excerpts from Leeds relied on by the Examiner only relate to a host computer associated with a sender of an electronic mail message (see Abstract and Col. 4, lines 66-67, specifically). In addition, Leeds discloses that "if a message has purportedly been relayed through a machine named mail.fromnowhere.com and the mail handling system has determined that such a machine does not actually exist, the confidence rating for the message should be increased." Clearly, determining a host computer/host name of a sender of e-mail or relay, as in Leeds, does not meet appellant's specific claim language, namely an "authority hosting the network address" (emphasis added), as claimed by appellant.

Further, appellant respectfully asserts that the excerpts from Aronson relied upon by the Examiner merely disclose that "[o]ther contemplated rule handling filter modules will filter e-mail based on: (1) word or letter frequency analysis; (2) IP source frequency analysis; (3) misspelling analysis (unwanted e-mail often contains misspelled words); (4) word or letter



combination analysis; (5) technical or legal RFC822 header compliance; and (6) feature extraction & analysis (e.g., based on phone numbers, URI's, addresses, etc.)" (emphasis added). Clearly, filtering e-mail based on IP source frequency and feature extraction & analysis fails to even suggest "identify[ing] an authority hosting the network address" (emphasis added), as claimed by appellant.

In addition, the Examiner argued that "Ar[on]son disclosed that the source header data from an incoming e-mail address (aardvark@aol.com) is analyzed by the spam probes." Further, the Examiner argued that "[t]he source header data includes the ISP (in this case "aol") hosting the spammer's network address (see col.4, lines 45-67)." Appellant disagrees and respectfully asserts that the excerpt from Aronson simply discloses that "[a] spam probe is an e-mail address selected to make its way onto as many spam mailing lists as possible." Aronson continues, teaching that "[i]t is also selected to appear high up on spammers' lists in order to receive spam mailings early in the mailing process" using an e-mail address such as "aardvark@aol.com." Clearly, the mere disclosure of using an e-mail address in a spam probe, as in Aronson, completely fails to even suggest "identify[ing] an authority hosting the network address" (emphasis added), as claimed by appellant.

Still with respect to independent Claim 22, the Examiner has again relied on the Abstract; Col. 3, lines 54-67; and Col. 4, lines 1-35 in Leeds to make a prior art showing of appellant's claimed "code that generates a report containing the identified network address."

Appellant respectfully asserts that the only suggestion of a "report" in the excerpts relied on by the Examiner merely relates to "seed addresses [which] can alert an e-mail provider to potential mass mailings by reporting when mail is received for ghost or non-existent accounts." Clearly, alerting an e-mail provider when an e-mail is received for a seed address, as in Leeds, fails to even suggest "generat[ing] a report containing the identified network address" (emphasis added), as claimed by appellant.

Further, the Examiner argued that "Leeds also describes the similar process of identifying the host name of the spammer's address (please see col.4, lines 60-67 & col.5, lines 1-45)." Appellant disagrees and respectfully asserts that Leeds simply discloses that "[t]he fields for

"Return Path:," "From:," and "Reply-To:" are highlighted as three of the fields which the present invention will parse from the message header.' As an example, Leeds teaches that "From: 48941493@notarealaddress.com is broken down into a user id (48941493) and a host name (notarealaddress.com)" (emphasis added). Leeds continues, disclosing that 'a first level check is [used] to determine if the alleged sender identified by the "From:" or "Reply-To:" fields are valid.' Moreover, Leeds discloses that the first level check 'includ[es]: (1) sending a message to the user identified by the "From:" or "Reply-To:" fields and examining whether the message can be successfully delivered, (2) using the UNIX "whois" command to determine if a site (or host) by that name actually exists, (3) using the UNIX "finger" command to identify if a user name exists at a verifiable host, (4) using the "vrfy" command when connected to a sendmail daemon to verify that a user exists at a particular site, and (5) using the UNIX "traceroute" command to make sure there is a valid route back to the specified host' (emphasis added). Clearly, performing a first level check including using whois, and traceroute to verify the host name from the "From:" and "Reply-To:" fields, as in Leeds, fails to even suggest "generat[ing] a report containing the identified network address" (emphasis added), as claimed by appellant.

Further, with respect to independent Claim 22, the Examiner has relied on Col. 4, lines 60-67; Col. 5, lines 1-44; and Col. 6, lines 52-65 in Leeds to make a prior art showing of appellant's claimed technique "wherein identifying the hosting authority comprises identifying an owner of a network domain."

Appellant respectfully asserts that the excerpts from Leeds relied upon by the Examiner merely disclose 'a first level check is to determine if the alleged sender identified by the "From:" or "Reply-To:" fields are valid' (emphasis added). In addition, Leeds discloses 'using the UNIX "whois" command to determine if a site (or host) by that name actually exists' (emphasis added). Clearly, using whois to perform a first level check to ensure the host actually exists for the alleged sender in the "From:" or "Reply-To:" fields, as in Leeds, fails to even suggest a technique "wherein identifying the hosting authority comprises identifying an owner of a network domain" (emphasis added), as claimed by appellant. Appellant respectfully asserts that merely ensuring that a host actually exists fails to even suggest "identifying an owner of a network domain," as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

*Group # 13: Claim 25*

With respect to Claim 25, the Examiner has relied on Col. 4, lines 57-67, Col. 5, lines 1-8, and Col. 5, lines 50-67 in Aronson to make a prior art showing of appellant's claimed "code that compares text within the electronic message to a database of words to locate the network address within the text."

After careful review of the excerpts relied on by the Examiner, appellant notes that Aronson merely discloses that "[i]f the network address contained in the source header is identified as the network address of a known spammer, a rule will be established to filter all incoming e-mail from this network address into the spam storage area 230" (Col. 4, lines 60-62 – emphasis added). Further, Aronson discloses that "[r]ules 210 based on keywords in the subject or body of spam e-mail may also be established" and "[f]or example, all e-mails containing the two words "sex" and "free" may be identified as spam and filtered" (Col. 4, lines 2-5 – emphasis added). In addition, Aronson discloses that "[o]ther contemplated rule handling filter modules will filter e-mail based on: (1) word or letter frequency analysis; (2) IP source frequency analysis; (3) misspelling analysis (unwanted e-mail often contains misspelled words); (4) word or letter combination analysis; (5) technical or legal RFC822 header compliance; and (6) feature extraction & analysis (e.g., based on phone numbers, URL's, addresses, etc.)" (Col. 5, lines 58-64 – emphasis added).

However, the mere disclosure that the network address contained within the source header is used by a rule to filter e-mail from this network address to a spam storage area, as in Aronson, simply fails to even suggest "code that compares text within the electronic message to a database of words to locate the network address within the text" (emphasis added), in the manner claimed by appellant. Further, Aronson's disclosure to identify and filter spam based on keywords in the subject or body fails to suggest "code that compares text within the electronic message to a database of words to locate the network address within the text" (emphasis added), as claimed by appellant. In addition, Aronson's disclosure that rule handling filter modules will filter e-mail

based on IP source frequency analysis, and feature extraction & analysis simply fails to suggest “code that compares text within the electronic message to a database of words to locate the network address within the text” (emphasis added), as claimed by appellant. Clearly, identifying and filtering spam based on keywords and features, as in Aronson, fails to meet “a database of words to locate the network address within the text” (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

*Group #14: Claim 26*

With respect to Claim 26, the Examiner has relied on Col. 4, lines 57-67; Col. 5, lines 1-8; and Col. 5, lines 50-67 in Aronson to make a prior art showing of appellant’s claimed “code that compares the identified network address with trusted network addresses.”

After careful review of the excerpts relied on by the Examiner, appellant notes that Aronson merely discloses that “[i]f the network address contained in the source header is identified as the network address of a known spammer, a rule will be established to filter all incoming e-mail from this network address into the spam storage area 230” (Col. 4, lines 60-62 – emphasis added).

However, appellant respectfully asserts that Aronson’s disclosure of filtering e-mail as spam based on the source address being identified as a known spammer simply fails to even suggest “code that compares the identified network address with trusted network addresses” (emphasis added), as claimed by appellant. Clearly, the source address of a known spammer, as in Aronson, simply fails to suggest “trusted network addresses” (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

*Group #15: Claim 29*

With respect to Claim 29, the Examiner has relied on Col. 4, lines 37-67; and Col. 5, lines 1-44 in Leeds to make a prior art showing of appellant's claimed technique "wherein the report is utilized to generate an electronic mail message to be sent to the identified organization."

Appellant respectfully asserts that Leeds merely discloses "automatically sending a reply (in the form of a verification request) to the purported sender(s)" (Col. 4, lines 38-40 – emphasis added). Further, Leeds discloses 'issuing a verification request and can be in many forms, including: (1) sending a message to the user identified by the "From:" or "Reply-To:" fields and examining whether the message can be successfully delivered' (Col. 5, lines 20-23 – emphasis added). However, such verification request message sent to users fails to meet a technique "wherein the report is utilized to generate an electronic mail message to be sent to the identified organization" (emphasis added), as claimed by appellant. Clearly, sending a verification message to the purported senders, as in Leeds, fails to meet "an electronic mail message to be sent to the identified organization" (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

*Group #16: Claim 30*

With respect to Claim 30, the Examiner has relied on Col. 4, lines 36-67; and Col. 5, lines 1-44 in Leeds to make a prior art showing of appellant's claimed technique "wherein identifying the URL further comprises examining text surrounding the URL to determine a likelihood that the URL is an address of a web site associated with unsolicited messages."

Appellant respectfully asserts that Leeds merely discloses that "previously read junk e-mail can be added to the rules base to look for certain phrases" and that "[t]his may not be sufficient, however, to screen out valid mail that cites or quotes from the junk e-mail." (Col. 4, lines 52-56 – emphasis added). Further, Leeds discloses that "[i]f, however, the content is combined with an address that cannot pass a verification request, the user may wish to assign a 100% confidence

rating, and the mail can optionally be automatically deleted” (Col. 4, lines 56-59). However, the mere disclosure of looking for certain phrases, as in Leeds, simply fails to even suggest a technique “wherein identifying the URL further comprises examining text surrounding the URL to determine a likelihood that the URL is an address of a web site associated with unsolicited messages” (emphasis added), as claimed by appellant. Clearly, looking for certain phrases fails to specifically suggest “examining text surrounding the URL” (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

*Group #17: Claim 31*

With respect to Claim 31, the Examiner has relied on Col. 4, lines 36-67; and Col. 5, lines 1-44 in Leeds to make a prior art showing of appellant’s claimed technique “wherein the report includes disclaimer information and user definable text.”

Appellant respectfully asserts that Leeds merely discloses “automatically sending a reply (in the form of a verification request) to the purported sender(s)” (Col. 4, lines 38-40 – emphasis added). Further, Leeds discloses “issuing a verification request and can be in many forms, including: (1) sending a message to the user identified by the “From:” or “Reply-To:” fields and examining whether the message can be successfully delivered” (Col. 5, lines 20-23 – emphasis added). However, such verification request message sent to users, as in Leeds, fails to even suggest a technique “wherein the report includes disclaimer information and user definable text” (emphasis added), as claimed by appellant. Clearly, the mere disclosure of a verification request fails to suggest “disclaimer information and user definable text” (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

## VIII CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A method for generating a report on an unsolicited electronic message, comprising:

receiving an electronic mail message;

determining whether the electronic message is an unsolicited message;

if the message is an unsolicited message,

examining the message to identify a network address relating to the message,

identifying an authority hosting the network address, and

generating a report containing the identified network address and hosting authority;

wherein identifying the hosting authority comprises identifying an owner of a network domain.

2. (Original) The method of claim 1 further comprising transmitting the generated report to the identified hosting authority.

3. (Original) The method of claim 1 wherein examining the message to identify a network address comprises identifying a URL.

4. (Original) The method of claim 3 wherein identifying a URL comprises comparing text within the electronic message to a database of words to identify the URL.

5. (Original) The method of claim 3 further comprising comparing the identified URL to a database of legitimate URLs.

6. (Original) The method of claim 5 further comprising updating the database based on electronic messages received.



7. (Original) The method of claim 3 wherein identifying the hosting authority comprises utilizing an Internet tool to locate a web server hosting the URL.

8. (Original) The method of claim 7 wherein utilizing an Internet tool comprises utilizing WHOIS.

9. (Cancelled)

10. (Original) The method of claim 1 wherein identifying the hosting authority comprises identifying an Internet service provider.

11. (Original) The method of claim 1 further comprising transmitting the report to a central managed service provider configured to forward the report to the identified hosting authority.

12. (Original) The method of claim 1 further comprising at least temporarily saving the report and transmitting the report to the identified hosting authority at the end of a specified period.

13. (Previously Presented) A system for generating a report on an unsolicited electronic message, the system comprising:

- a detector operable to detect a network address within an electronic message identified as an unsolicited message;

- a host identifier operable to identify an authority hosting the network address;

- a report generator operable to generate a report containing the identified network address and hosting authority; and

- a storage medium configured to at least temporarily store the identified network address and hosting authority;

- wherein identifying the hosting authority comprises identifying an owner of a network domain.

14. (Original) The system of claim 13 further comprising a detector operable to detect unsolicited messages.

15. (Original) The system of claim 13 wherein the network address is a URL.

16. (Original) The system of claim 13 wherein the hosting authority is an Internet service provider.

17. (Original) The system of claim 13 further comprising a processor operable to transmit the generated report.

18. (Original) The system of claim 17 wherein the processor is configured to transmit the report to the identified hosting authority.

19. (Original) The system of claim 17 wherein the processor is configured to transmit the report to a central managed service provider.

20. (Original) The system of claim 13 further comprising a database containing search terms used to identify the network address within text of the electronic message.

21. (Original) The system of claim 13 further comprising a database containing a list of trusted network addresses.

22. (Previously Presented) A computer product for generating a report on an unsolicited electronic message, comprising:

- code that receives an electronic mail message;
- code that determines whether the electronic message is an unsolicited message;
- code that examines the message to identify a network address relating to the message if the message is an unsolicited message,
- code that identifies an authority hosting the network address;
- code that generates a report containing the identified network address; and
- a computer readable medium that stores said computer codes;

wherein identifying the hosting authority comprises identifying an owner of a network domain.

23. (Original) The computer product of claim 22 wherein the computer readable medium is selected from the group consisting of CD-ROM, floppy disk, tape, flash memory, system memory, hard drive, and a data signal embodied in a carrier wave.

24. (Original) The computer product of claim 22 further comprising code that transmits the generated report to the identified hosting authority.

25. (Original) The computer product of claim 22 further comprising code that compares text within the electronic message to a database of words to locate the network address within the text.

26. (Original) The computer product of claim 22 further comprising code that compares the identified network address with trusted network addresses.

27. (Previously Presented) The method of claim 1 wherein identifying the hosting authority further comprises identifying an address, an administrative contact name, an administrative contact telephone number, and a name of at least one server associated with the hosting authority.

28. (Previously Presented) The method of claim 1 wherein identifying the hosting authority further comprises identifying an organization to which the network domain is registered.

29. (Previously Presented) The method of claim 28 wherein the report is utilized to generate an electronic mail message to be sent to the identified organization.

30. (Previously Presented) The method of claim 4, wherein identifying the URL further comprises examining text surrounding the URL to determine a likelihood that the URL is an address of a web site associated with unsolicited messages.

31. (Previously Presented) The method of claim 1 wherein the report includes disclaimer information and user definable text.

**IX EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))**

There is no such evidence.

**X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))**

N/A

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NA11P314).

Respectfully submitted,

By: /KEVINZILKA/

Date: March 8, 2007

Kevin J. Zilka  
Reg. No. 41,429

Zilka-Kotab, P.C.  
P.O. Box 721120  
San Jose, California 95172-1120  
Telephone: (408) 971-2573  
Facsimile: (408) 971-4660



## UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22111-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/072,708	02/05/2002	Luke David Jagger	NETAP021	1914

2KX75 7540 02/08/2007

Zilka-Kotab, PC  
P.O. BOX 721120  
SAN JOSE, CA 95172-1120

EXAMINER

ART UNIT

PAPER NUMBER

DATE MAILED: 02/08/2007

Please find below and/or attached an Office communication concerning this application or proceeding.



**Notification of Non-Compliant Appeal Brief  
(37 CFR 41.37)**

Application No.

10/072,708

Applicant(s)

JAGGER ET AL.

Examiner

Asghar Bilgrami

Art Unit

2143

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

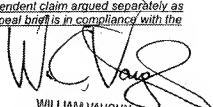
The Appeal Brief filed on 11 December 2006 is defective for failure to comply with one or more provisions of 37 CFR 41.37.

To avoid dismissal of the appeal, applicant must file an amended brief or other appropriate correction (see MPEP 1205.03) within **ONE MONTH or THIRTY DAYS** from the mailing date of this Notification, whichever is longer.

**EXTENSIONS OF THIS TIME PERIOD MAY BE GRANTED UNDER 37 CFR 1.136.**

1. ☐ The brief does not contain the items required under 37 CFR 41.37(c), or the items are not under the proper heading or in the proper order.
2. ☐ The brief does not contain a statement of the status of all claims, (e.g., rejected, allowed, withdrawn, objected to, canceled), or does not identify the appealed claims (37 CFR 41.37(c)(1)(iii)).
3. ☐ At least one amendment has been filed subsequent to the final rejection, and the brief does not contain a statement of the status of each such amendment (37 CFR 41.37(c)(1)(iv)).
4. ☒ (a) The brief does not contain a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by page and line number and to the drawings, if any, by reference characters; and/or (b) the brief fails to: (1) identify, for each independent claim involved in the appeal and for each dependent claim argued separately, every means plus function and step plus function under 35 U.S.C. 112, sixth paragraph, and/or (2) set forth the structure, material, or acts described in the specification as corresponding to each claimed function with reference to the specification by page and line number, and to the drawings, if any, by reference characters (37 CFR 41.37(c)(1)(v)).
5. ☐ The brief does not contain a concise statement of each ground of rejection presented for review (37 CFR 41.37(c)(1)(vi)).
6. ☐ The brief does not present an argument under a separate heading for each ground of rejection on appeal (37 CFR 41.37(c)(1)(vii)).
7. ☐ The brief does not contain a correct copy of the appealed claims as an appendix thereto (37 CFR 41.37(c)(1)(viii)).
8. ☐ The brief does not contain copies of the evidence submitted under 37 CFR 1.130, 1.131, or 1.132 or of any other evidence entered by the examiner and **relied upon by appellant in the appeal**, along with a statement setting forth where in the record that evidence was entered by the examiner, as an appendix thereto (37 CFR 41.37(c)(1)(ix)).
9. ☐ The brief does not contain copies of the decisions rendered by a court or the Board in the proceeding identified in the Related Appeals and Interferences section of the brief as an appendix thereto (37 CFR 41.37(c)(1)(x)).
10. ☒ Other (including any explanation in support of the above items):

"Summary of claimed subject matter" does not contain brief explanation of any dependent claim argued separately as required by (37 CFR 41.37(c)(1)(v)). Applicant is encouraged to verify that the appeal brief is in compliance with the requirements stipulated in the MPEP.

  
WILLIAM VAUGHN  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100